UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/053,703	01/24/2002	Joel Maurin	T2147-907679	7844

181 7590 06/01/2007

MILES & STOCKBRIDGE PC
1751 PINNACLE DRIVE
SUITE 500
MCLEAN, VA 22102-3833

EXAMINER	
OKORONKWO, CHINWENDU C	
ART UNIT	**PAPER NUMBER**
2136	
MAIL DATE	**DELIVERY MODE**
06/01/2007	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/053,703	MAURIN ET AL.	
	Examiner	Art Unit	
	Chinwendu C. Okoronkwo	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 February 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Priority

1. Acknowledgment is made of applicant's claim for foreign priority under 35 U.S.C. 119(a)-(e). The certified copy has been filed in parent Application No. 0100946 (France), filed on 01/24/2001.

Information Disclosure Statement

2. For the record, the Examiner acknowledges that the IDS submitted on 10/06/2005. It has been received and considered.

Oath/Declaration

3. For the record, the Examiner acknowledges that the Oath/Declaration submitted on 01/24/2002 has been received and considered.

Drawings

4. For the record, the Examiner acknowledges that the Drawings submitted on 01/24/2002 have been received and considered.

Specification

5. For the record, the Examiner acknowledges that the Specification submitted on 01/24/2002 has been received and considered.

Response to Remarks/Arguments

6. In response to communications filed on 02/28/2007, applicant amends claims 1, 3, 4 and 6-8; cancels claim 5. The following claims, claims 1-4 and 6-8, are presented for examination.

6.1 Applicant's arguments, pages 6-8, with respect to the rejection of claims 1-4 and 6-8 have been fully considered but they are not persuasive.

Amongst other adjustments the Examiner encourages the Applicant to further detail the definition and explanation of within the claim limitations "cookie" and "cookie header" to further reflect the intended understanding and disclosure within the Specification. The Examiner understands the disclosure of Devine to clearly disclose the claimed invention as explained in the previous Office Actions. The remarks and arguments of the Applicant serve to argue that the Devine and Grantges disclosures do not constitute a cookie header without providing evidence of the differences between the claimed invention and disclosed invention – specifically which elements are and are not disclosed with regards to the respective references. The Devine reference discloses a cookie jar server 32 that "generate[s] a 'cookie' or session identifier which is a unique server-generated key that is sent to the client along with each reply to a HTTPS request (column 8 lines 44-60 of Devine)." The further disclosure that the cookie jar goes through its stored list of cookies, identifies the cookie for the session and returns the cookie to the Web server again by means of HTTPS message (column

19 lines 24-33 of Devine) combined with Grantges disclosure of several cookies created by a gateway proxy server: an authentication cookie, an applications list cookie, and a selected-application cookie (column 9 lines 54-56 and Figure 4A of Grantges) provides clear evidence of the disclosure of the claimed invention, not merely with regards to claim language but also in regards to the functionality of objective goal of the claimed invention – specifically the cookie header containing a plurality of cookies. Additionally, the Examiner submits that the topic of feasibility and enablement of the claimed invention has been raised on several discussions of the case with more experienced Primary Examiners and a Supervisory Patent Examiner – specifically the recursive concept of a cookie header containing a plurality of cookies, each of which is (based upon the broadest interpretation) understood to be of the same type of cookie, thus also containing within its header a plurality of cookies.

Based upon the above reasoning the rejections of claims 1-8 are maintained. The Applicant has failed to overcome the rejections.

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-8 rejected under 35 U.S.C. 103(a) as being unpatentable over Devine et al. (US Patent No. 6,598,167) and further in view of Grantges et al. (US Patent No. 6,510,464).

Regarding claim 1, Devine et al., discloses a method of communicating to a server machine a certificate of a user which is sent by a client machine via a security module of a computer system, wherein a first protocol used between the client machine and the server machine is a stateless protocol, and a second protocol used between the client machine and the security module is a stateless protocol, said method comprising:

transmitting the request, including said cookie header containing said certificate, from the security module to the server machine, wherein said certificate has a plurality of separators; and wherein said cookie header includes a plurality of cookies (0029,0066,0083,0130 and 0131).

Devine et al. is silent in disclosing inserting said certificate into a cookie header of a request in the first protocol, however Grantges et al. doses disclose this limitation (col. 2 lines 36-54 and col. 10 lines 6-31). It would have been obvious for one of ordinary skill in the art, at the time of the invention, to combine the secure gateway having routing feature of Grantges et al. with the secure customer interface for web based data management of Devine et al. Grantges et al. provide motivation for this combination in the recitation, "In a preferred

embodiment, the identifier comprises a character string associate with the application to which the user of the remote client computer is provided access. The gateway is configured to create a cookie containing the identifier wherein subsequent requests made by the client computer also include the cookie containing the identifier. Through the foregoing, the identification of the selected application is known by the gateway (col. 3 lines 21-29 of Grantges et al.)." Therefore it would have been obvious to combine these concepts as it is the preferred manner of provided increased security to transmitted messages.

Regarding claim 2, Devine et al., discloses method according to claim 1, further comprising: removing from said certificate all separators used in headers of the request prior to insertion of said certificate into said cookie header (0131 of Devine et al.).

Regarding claim 3, Devine et al., discloses a method according to claim 1, wherein said inserting step further comprises: determining, prior to the inserting step, whether an existing cookie header is present in the request sent by the client machine; and creating a new cookie header if said existing cookie header is not present in the request sent by the client machine (0124 of Devine et al.).

Regarding claim 4, Devine et al., is silent in disclosing a method according to claim 3, further comprising: adding a specific cookie into the existing or new

cookie header; and assigning a configurable default name to said specific cookie to enable the server machine to distinguish the certificate from cookies of the request, however Grantges et al. doses disclose this limitation (col. 2 lines 36-54 and col. 10 lines 6-31). It would have been obvious for one of ordinary skill in the art, at the time of the invention, to combine the secure gateway having routing feature of Grantges et al. with the secure customer interface for web based data management of Devine et al. Grantges et al. provide motivation for this combination in the recitation, "In a preferred embodiment, the identifier comprises a character string associate with the application to which the user of the remote client computer is provided access. The gateway is configured to create a cookie containing the identifier wherein subsequent requests made by the client computer also include the cookie containing the identifier. Through the foregoing, the identification of the selected application is known by the gateway (col. 3 lines 21-29 of Grantges et al.)." Therefore it would have been obvious to combine these concepts as it is the preferred manner of provided increased security to transmitted messages.

Regarding claim 6, Devine et al., is silent in disclosing a security machine which secures exchanges between a client machine and a server machine of a computer system, wherein a first protocol used between the client machine and server machine is a stateless protocol, and a second protocol is implemented between the client machine and said security machine is a stateless protocol,

said security machine is comprising: an analyzer which enables the transmission of a certificate inserted into a cookie header of an HTTP or equivalent request wherein said cookie header includes a plurality of cookies (0130 and 0131 of Devine et al.).

Regarding claim 7, Devine et al., discloses a system comprising:
a client machine, a server machine, and a security module (0029, 0066, 0083, 0130 and 0131 of Devine et al.).

Devine et al., is silent in disclosing a first protocol used between the client machine and the server machine are configured to communicate using a first protocol, said first protocol comprising a stateless protocol; wherein the client machine and the security module are configured to communicate using a second protocol, said second protocol comprising a secure stateless protocol; and wherein the security module comprises an analyzing program which enables transmission of a certificate sent by the client machine in a cookie header of a request in said stateless protocol, whereto stud cookie header includes a plurality of cookies, however Grantges et al. doses disclose this limitation (col. 2 lines 36-54 and col. 10 lines 6-31). It would have been obvious for one of ordinary skill in the art, at the time of the invention, to combine the secure gateway having routing feature of Grantges et al. with the secure customer interface for web based data management of Devine et al. Grantges et al. provide motivation for

this combination in the recitation, "In a preferred embodiment, the identifier comprises a character string associate with the application to which the user of the remote client computer is provided access. The gateway is configured to create a cookie containing the identifier wherein subsequent requests made by the client computer also include the cookie containing the identifier. Through the foregoing, the identification of the selected application is known by the gateway (col. 3 lines 21-29 of Grantges et al.)." Therefore it would have been obvious to combine these concepts as it is the preferred manner of provided increased security to transmitted messages.

Regarding claim 8, Devine et al., a computer readable medium upon which is embodied a sequence of programmable instructions which, when executed by a security module of a computer system, cause the security module to perform operations comprising: communicating to a server machine a certificate of a user which is sent by a client machine via the security module, wherein a first protocol used between the client machine and the server machine is a stateless protocol, and wherein a second, protocol used between the client machine and the security module is a secure stateless protocol; inserting said certificate into a cookie header of a request in the first protocol; and transmitting the request, including said cookie header containing said certificate, from the security module to the server machine; wherein said certificate has a plurality of separators; and

wherein said cookie header includes a plurality of cookies (0029, 0066, 0083, 0130, 0131 and 0149 of Devine et al.).

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Chinwendu C. Okoronkwo whose telephone number is (571) 272 2662. The examiner can normally be reached on MWF 9:30 - 7:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Nasser Moazzami can be reached on (571) 272 4195. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

CCO

May 28, 2007

NASSER MOAZZAMI
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

5/29/07